Beschreibung
des Aktivierungsvorgangs eines LoRa Device

Version: 1.2

Stand: 26.06.2018

Inhaltsverzeichnis:

1 Was ist LoRa?

LoRa ist ein Long Range Funk bei dem jede 0 und 1 die übertragen werden soll als ein Frequenzmuster übertragen wird (Spreizverfahren). Das verlängert zwar die Protokolllänge also auch die Übertragungszeit kann aber über spezielle Verfahren auch als extrem schwaches Signal noch gefiltert und empfangen werden. Entwickelt hat es die Firma Semtec. LoRa eignet sich nur zur Übertragung geringer Datenmengen pro Zeiteinheit.

1.1 Was ist LoRa-Wan?

Die Firma IBM hat ein Netzwerkprotokoll speziell für Funk IoT entworfen. LoRa wurde als geeignetes Übertragungsverfahren ausgewählt, und so ist LoRa-Wan entstanden. LoRa-Wan ist Bi-direktional und gibt es in Class A, B und C.
Im Mode Class A ist das LoRa Gerät asynchron zum Netz. Im Class B Mode hält das Gerät über kurze Synchronisationsfenster sich synchron zum Netz. Im Modus Class C ist das Gerät per Funk immer mit dem Netz verbunden. Die notwendige Energie zum Betreiben steigt von A nach C, C ist nur netzbetrieben sinnvoll möglich.

2 Aufbau eines LoRa Wan Netzwerkes

Das LoRa-Wan Netzwerk ist ein Stern-Netz aus einem oder mehreren Sternpunkten. Die Sternpunkte nennt man Gateway. Diese sind über ein IP-Netzwerk mit einem Netzwerkserver verbunden. Der Netzwerk-Server besteht real aus mehreren Servern. Der Server für die Organisation der Kommunikation im Netzwerk, dem Sicherheits-Server welcher für die Registrierung und die Schlüsselverwaltung zuständig ist und den Applikations-Server. Dieser ist dann der Teil der die Nutzdaten entschlüsselt und dann weiter verarbeitet.
Ein LoRa-Wan Netzwerk kann von einem Provider betrieben und deren Nutzung verkauft werden oder man kann ein oder mehrere eigene Netzwerke betreiben. Dabei können die Netzwerke als „public“ oder „privat“ deklariert werden.

2.1 Wo sitzt der Netzwerkserver?

Der Netzwerk-Server kann in Mini-Netzen in dem einen Gateway des Netzwerkes mit betrieben werden. Im Normalfall aber auf einem separatem Rechner oder auch Raspberry-Pi. Das Netzwerk besteht dann zumeist aus 1-n Gateways welche in dem Empfangsgebiet sinnvoll verteilt angebaut werden. Je höher die Anbaulage, des so besser der Empfang also auch die Reichweite.

2.2 Wo kommen die Nutzdaten an?

Die Nutzdaten also die Applikationsdaten sind extra mit einem Schlüssel verschlüsselt. Diesen kennt im Normalfall nur der Applikations-Server. Der Applikationsserver sollte aus Sicherheitsgründen auf einem extra System laufen.

3 Wer speichert die Nutzdaten?

Der Applikationsserver kann die Daten entschlüsseln und dann interpretieren. Es gibt keine Regeln oder Normen wie die Datenformate aufgebaut sein müssen. Der Applikationsserver kann dann die Daten verarbeiten und oder auch speichern.

4 Begriffe

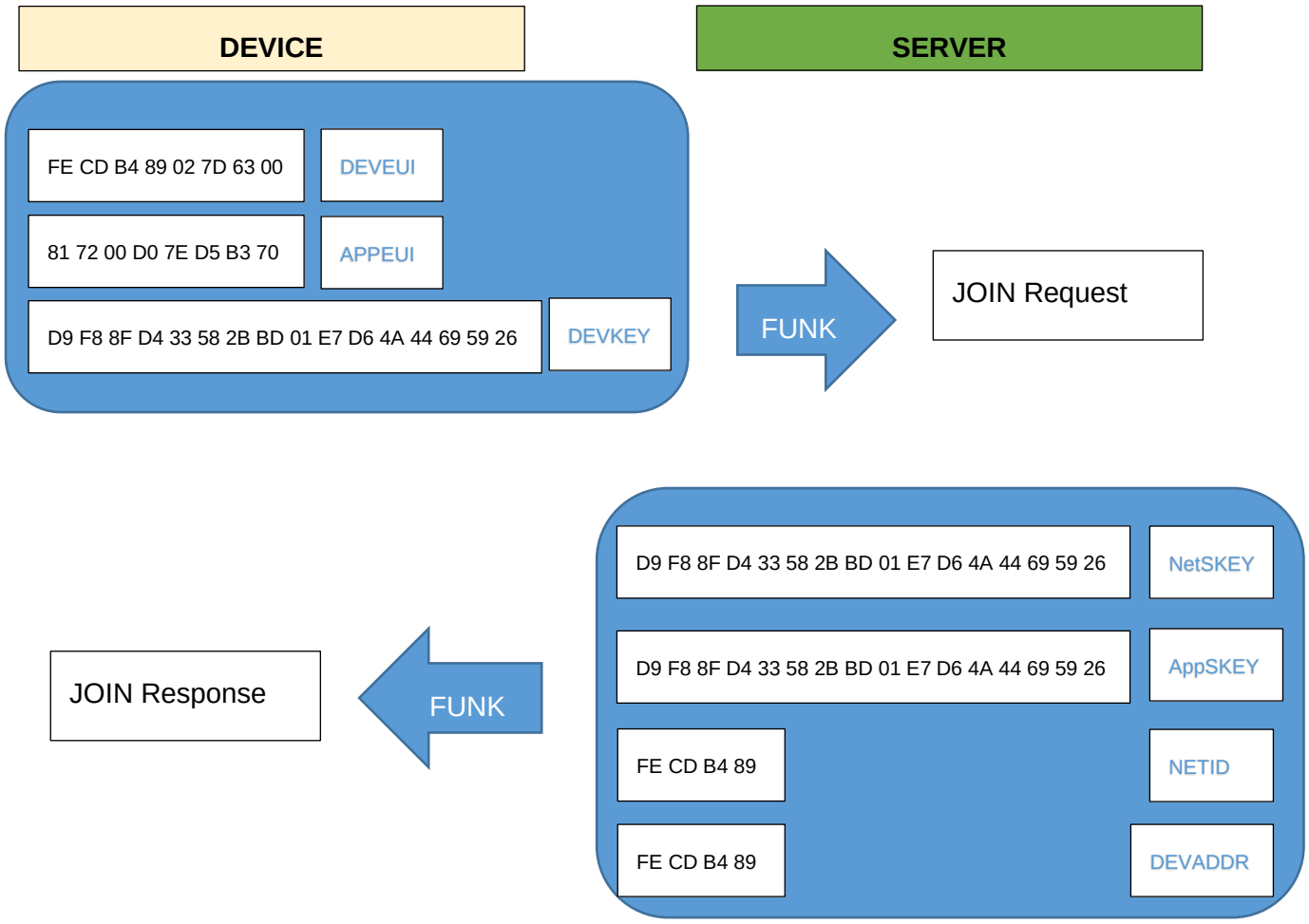
Net ID:	Nummer des LoRa-Wan Netzwerkes bei dem sich ein Device angemeldet hat.
DEVEUI:	Eindeutige und einmalige Kennung eines jeden Device. (ab Werk)
APPEUI:	Eindeutige und einmalige Kennung eines jeden Typs von Anwendung auf jeden Server
DEVKEY/ APPKEY:	öffentlicher Schlüssel für den Anmeldeprozess beim Server.
NetSKEY:	privater Schlüssel zum Verschlüsseln aller übertragenen Daten
AppSKEY:	privater Schlüssel des Anwenders um seine Nutzdaten zu Verschlüsseln
DEVADDR:	Nummer des registrierten Device nach einer Registrierung auf dem Server

5 Wie melde ich ein LoRa Device am Netzwerk an?

Jedes Gerät also Device muss sich beim Netzwerk anmelden um es nutzen zu können. Nach einer Anmeldung haben sich der Server und das Device miteinander bekannt gemacht und haben beide die richtigen Schlüssel für die Nutzdaten-Verschlüsselung und die Verschlüsselung der ganzen Protokolle. Dabei unterscheidet man zwischen den Verfahren OTAA und ABP.

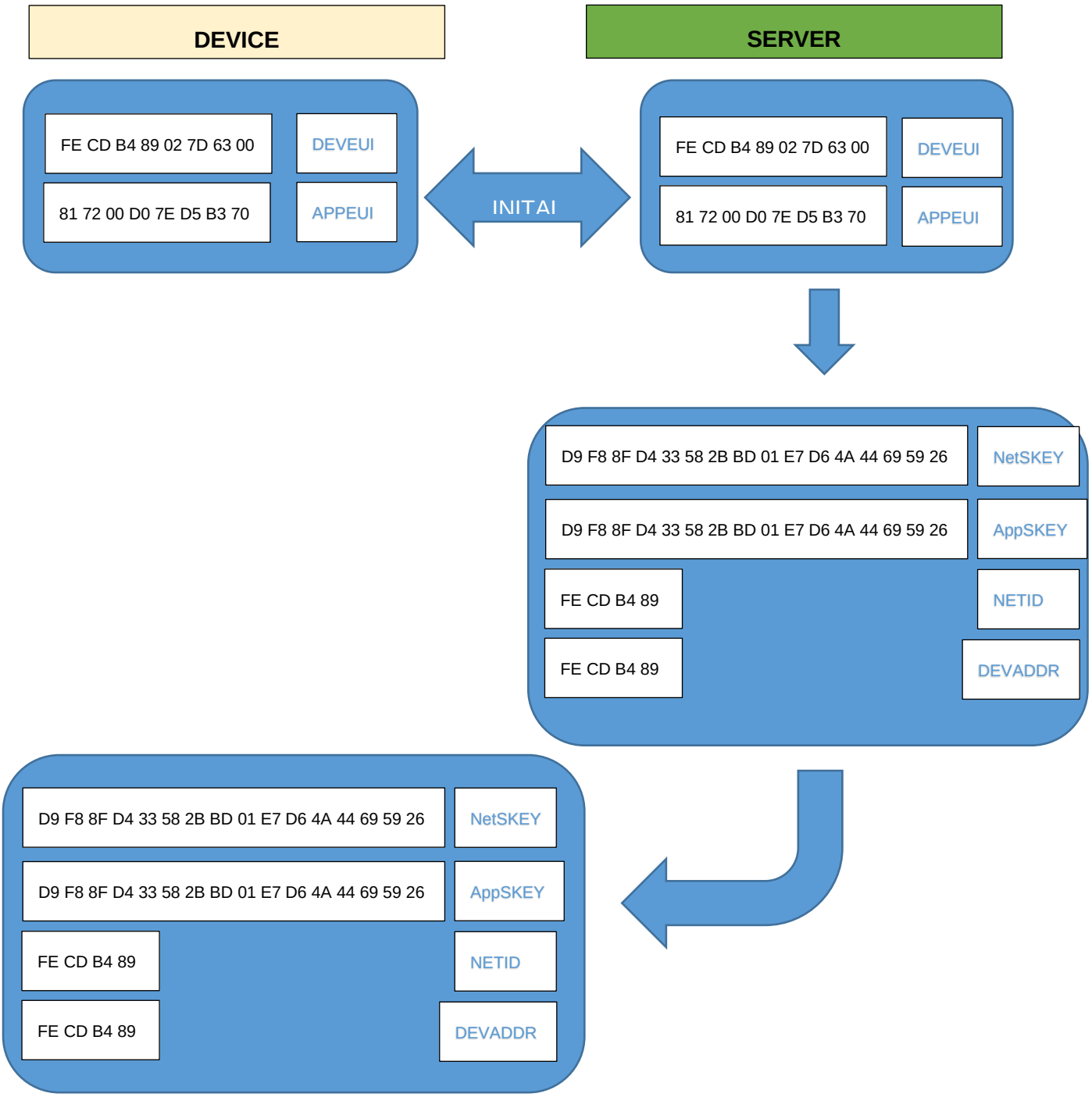
5.1 Was ist OTAA?

Bei OTAA sendet das Device nach einer Aktivierung eine Anfrage aus, ein Request. Das Device sendet dabei seine DEVEUI, die APPEUI und den DEVKEY. Wird die Anfrage von einem Netzwerkserver empfangen dem dieses Gerät und die Applikationskennung bekannt ist und der das auch noch mit dem richtigen DEVKEY, so antwortet der Server dem Gerät und teilt dem Server die NetID des Netzes, die DEVADDR unter der das Gerät ab nun auf dem Server gelistet ist und die entsprechenden AppSKEY und NetSKEY mit.



5.2 Was ist ABP?

Bei dem Verfahren ABP übernimmt der Mensch das Verbinden und Austauschen der Nummern. Auf dem Server wird das Gerät mit der entsprechenden DEVEUI und APPEUI schon angelegt. Der Server erstellt die NetSKEY und AppSKEY. Diese trägt der Anwender dann in das Device ein, inklusive der NetID des Netzes und der DEVADDR. Das Gerät braucht dann nach der Aktivierung nur anfangen zu senden. Es ist dem Netzwerk dann also schon bekannt.



5.3 Vorteile / Nachteile Einbindeverfahren

ABP

Vorteile:

- Gerät ist vorkonfektioniert und kann einfach nach dem Aktivieren mit senden beginnen

Nachteile:

- Vor Anbau der Geräte meist bei der Fertigung werden die Geräte schon vorkonfektioniert. Dazu müssen dem Fertiger alle Nummern schon vom Auftraggeber bereitgestellt werden.
  PROBLEM: Die DEVEUI wird erst bei der Fertigung erstellt ist aber für die Generierung und Bereitstellung der NetSKEY und AppSKEY notwendig.
  LÖSUNG: Der Kunde parametriert sich alle Geräte vor Anbau und Aktivierung selbst.
- Das Gerät kann sich bei keinem anderen Server mehr anmelden.

OTAA

Vorteile:

- Das Gerät kann sich bei verschiedenen Netzwerken anmelden wenn es dem Server bekannt ist.
- Bei der Fertigung wird die DEVEUI festgelegt und es benötigt keiner weiteren Parameter.

Nachteile:

- Vor Anbau der Geräte muss das Gerät dem Server bekannt gemacht werden und die vom Server generierten DEVKEY und der festgelegte APPKEY einprogrammiert werden.

5.4 Mögliche Szenarien als Lösung für die Parametrierung vor Anbau bzw. Aktivierung

Beide Varianten haben den Nachteil das bestimmte Nummern beiden Teilen, Server und Endgerät, bekannt sein müssen.

- Bei der Variante das der Kunde alles vorher auf seinem Server automatisch generiert hat und bei der Bestellung beim Produzenten mit bereitstellt, muss der Produzent alle Nummern wie DEVEUI, NetSKEY, AppSKEY, NETID, DEVADDR bei der Fertigung schon in das Gerät einschreiben. Nach einer Aktivierung bei Anbau beginnt das Gerät zu senden.
- Die universellste Lösung ist eine interaktive Aktivierung bei Anbau. Dabei liest der Monteur mit einem Optokopf und einem Mobile das Gerät aus (DEVEUI). Das App auf dem Mobile sendet die Daten an den Netzwerk-Server bzw. einem Server als Bindeglied zum Netzwerk-Server und dem Mobile-App. Dort wird automatisiert das Device auf dem Netzwerk-Server angelegt mit der entsprechenden APPEUI. Der Netzwerk-Server liefert als Ergebnis den DEVKEY und sendet diesen zum Mobile-App. Das Mobile schreibt über Optokopf diese Daten in das Device und aktiviert das Device per Kommando über den Optokopf. Das Device beginnt mit JOINREQUEST an den Netzwerk-Server. Wenn das Device sich verbunden hat kann das Mobile-App vom Netzwerk-Server direkt über eine MQTT-Schnittstelle erfahren ob das JOIN funktioniert hat.
- Für den Fall das ein LoRa-Server betrieben wird, der es erlaubt, dass der DEVKEY vom Anwender vorgegeben werden kann, ist es möglich sich bei der Bestellung auf einen APPEUI festzulegen. Jedes Gerät bekommt vom Hersteller eine eigene DEVEUI, jeder denselben APPEUI und jedes Gerät eine individuellen DEVKEY. Der Kunde bekommt dann

vom Hersteller eine Datei geliefert die eine Liste aller Geräte mit DEVEUI, APPEUI, DEVKEY beinhaltet. Der Kunde kann dann vor Anbau über einen automatisierten Prozess die Geräte dem Netzwerk-Server bekannt machen.